TD10 - Révisions de Cryptanalyse

Responsable : M. Bombar

1 Introduction

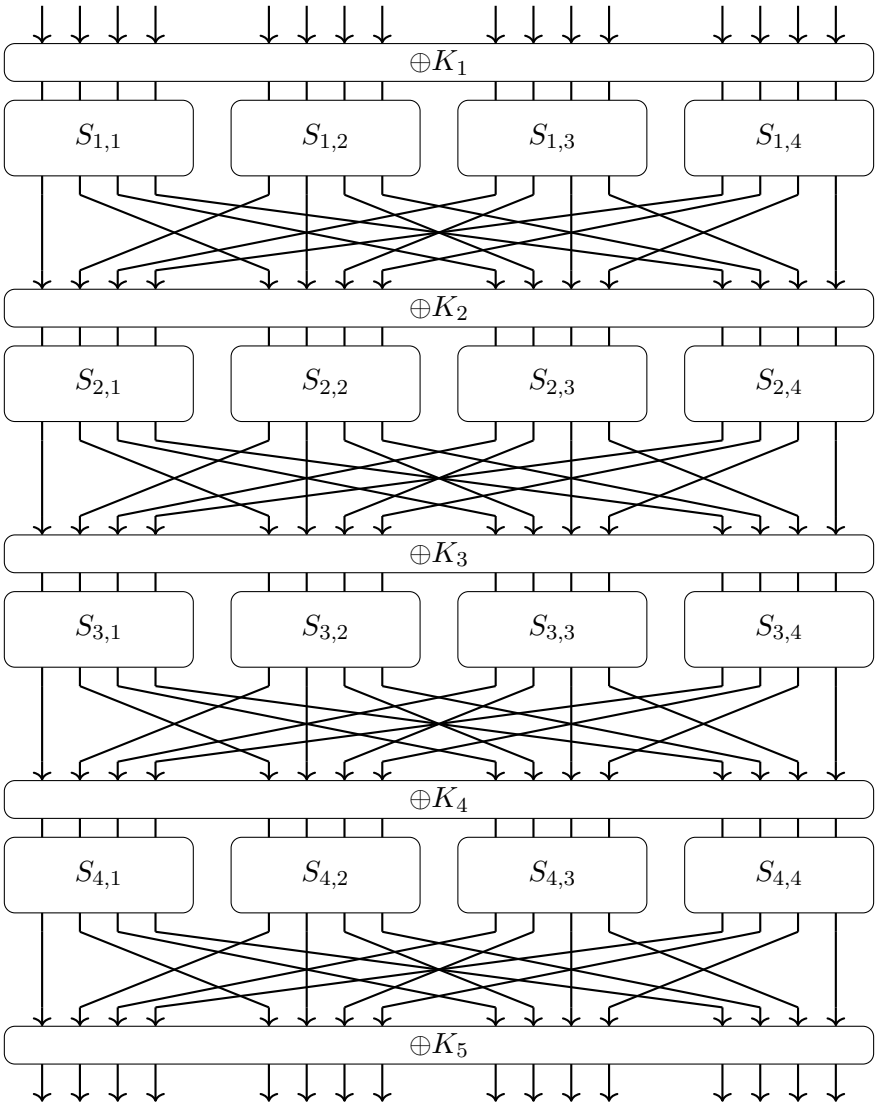


FIGURE 1 – Chiffrement par blocs de type SPN

On suppose que les boîtes S sont sur 4 bits par la Table 1

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(x)$	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7

TABLE 1 – Représentation de la boîte S (en hexadécimal)

La couche linéaire de diffusion pour chaque tour est une simple permutation linéaire des bits. Elle est représentée graphiquement en Figure 1 ainsi que dans la Table 2.

input	1	2	3	4	5	6	7	8	9	10	11	12	12	14	15	16
output	1	5	9	13	2	6	10	14	3	7	11	15	4	8	12	16

TABLE 2 – Permutation

2 Cryptanalyse Linéaire

2.1 Approximation des boîtes S

On rappelle la définition de la table des approximations linéaires d'une boîte S.

Définition

Pour chaque masque linéaire (α, β), on définit

$$\mathrm{LAT}[\alpha][\beta] = \sigma_{\alpha,\beta} - 2^{n-1} = 2^{n-1}\varepsilon_{\alpha,\beta}.$$

où

$$\sigma_{\alpha,\beta} = \#\Big\{\mathbf{x} \mid \langle\alpha, \mathbf{x}\rangle + \langle\beta, S(\mathbf{x})\rangle = 0\Big\}$$

est le nombre de solutions à l'approximation linéaire et

$$\mathbb{P}_{\mathbf{x}}\Big(\langle\alpha, \mathbf{x}\rangle + \langle\beta, S(\mathbf{x})\rangle = 0\Big) \stackrel{\text{def}}{=} \frac{\sigma_{\alpha,\beta}}{2^2} = \frac{1}{2}\big(1 + \varepsilon_{\alpha,\beta}\big)$$

(Q1) Construire une table des approximations linéaires de S.

(Q2) Quelle est le biais le plus probable ?

(Q3) Donner un masque (α, β) qui l'atteint.

2.2 Approximation Linéaire du Chiffré

On souhaite maintenant obtenir une approximation linéaire liant le texte clair avec l'entrée du 4ème tour. On souhaite que ça n'active que peu de bits de la clé pour pouvoir bénéficier de l'attaque.

Pour une boîte S donnée, on note X_1, X_2, X_3, X_4 ses entrées et Y_1, Y_2, Y_3, Y_4 ses sorties.

On considère le chemin linéaire suivant : $(1011, 0100) \to (0100, 0100) \to (0100, 0101)$ sur les boîtes $S_{1,2}, S_{2,2}, S_{3,2}$ (on l'obtient en lisant la permutation).

(Q4) Quelle est la probabilité que $X_1 \oplus X_3 \oplus X_4 = Y_2$ pour $S_{1,2}$?

(Q5) Quelle est la probabilité que $X_2 = Y_2 \oplus Y_4$ pour $S_{2,2}$?

(Q6) Quelle est la probabilité que $X_2 = Y_2 \oplus Y_4$ pour $S_{3,2}$?

Pour tout i on note U_i (respectivement V_i) le bloc de 16 bits de l'entrée de la boîte S du tour i, et pour tout j on note $U_{i,j}$ (resp. $V_{i,j}$) le j-ème bit (numeroté de 1 à 16 de gauche à droite). Par exemple, si P désigne le texte clair, on a $U_1 = P \oplus K_1$.

(Q7) Sous l'hypothèse que les approximations linéaires sont indépendantes, démontrer que la relation linéaire

$$V_{2,6} \oplus V_{2,8} \oplus P_5 \oplus P_7 \oplus P_8 \oplus K_{1,5} \oplus K_{1,7} \oplus K_{1,8} \oplus K_{2,6} = 0 \tag{1}$$

se produit avec probabilité $3/8$.

(Q8) Démontrez que

$$V_{3,6} \oplus V_{3,8} = U_{3,6}$$

et

$$V_{3,14} \oplus V_{3,16} = U_{3,14}$$

se produisent toutes les deux avec probabilité $3/4$.

(Q9) Montrer que

$$V_{3,6} \oplus V_{3,8} \oplus V_{3,14} \oplus V_{3,16} \oplus V_{2,6} \oplus K_{3,6} \oplus V_{2,8} \oplus K_{3,14} = 0 \tag{2}$$

avec probabilité $5/8$.

(Q10) En combinant (1) et (2), montrer que

$$U_{4,6} \oplus U_{4,8} \oplus U_{4,14} \oplus U_{4,16} \oplus P_5 \oplus P_7 \oplus P_8 \oplus \Sigma_K = 0$$

avec biais $-1/32$, où

$$\Sigma_K = K_{1,5} \oplus K_{1,7} \oplus K_{1,8} \oplus K_{2,6} \oplus K_{3,6} \oplus K_{3,14} \oplus K_{4,6} \oplus K_{4,8} \oplus K_{4,14} \oplus K_{4,16}.$$

Puisque les additions de clé ne change pas la magnitude du biais, on en déduit que

$$U_{4,6} \oplus U_{4,8} \oplus U_{4,14} \oplus U_{4,16} \oplus P_5 \oplus P_7 \oplus P_8 = 0$$

a lieu avec biais $\pm 1/32$.

2.3 Extraire les bits de la clé

(Q11) Rappeler comment monter une attaque de dernier tour.

3 Exercices sur les fonctions de hachage

3.1 Résistance aux collisions n'implique pas résistance aux préimages

Soit $h : \{0,1\}^\star \to \{0,1\}^n$ une fonction de hachage qu'on suppose **résistante aux collisions**. On construit la fonction de hachage suivante

$$h' : \begin{cases} \{0,1\}^\star & \to & \{0,1\}^{n+1} \\ x & \mapsto & \begin{cases} 0||x & \text{si } |x| = n. \\ 1||h(x) & \text{sinon.} \end{cases} \end{cases}$$

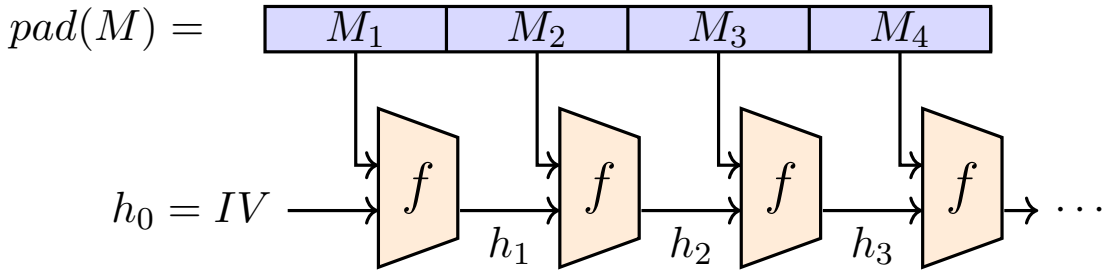
(Q12) Montrez que h' est résistante aux collision.

(Q13) Rappelez la définition formelle de la résistance à la préimage.

(Q14) Montrez que h' n'est pas résistante à la préimage.

3.2 Length-Extension Attack sur la construction de Merkle-Damgård

Soit H une fonction de hachage construite selon la méthode de Merkle-Damgård (par exemple MD5, SHA1, SHA256), dont on rappelle la construction ci-dessous.



(Q15) Soit $h = H(m) \in \{0,1\}^n$ le hash d'un message $m \in \{0,1\}^\star$ considéré comme secret. Soit $\sigma \in \{0,1\}^\star$ un suffixe quelconque (choisi par l'attaquant). Montrez qu'il est possible d'obtenir efficacement le hash d'un message étendu de la forme $m||padding||\sigma$ en temps $O(|\sigma|)$.

Indication : Supposer dans un premier temps que le message est de la bonne longueur, c'est-à-dire qu'il n'y a pas de *padding* interne.

(Q16) On considère un client C et un serveur S ayant partagé une clé secrète sk (par exemple à l'aide d'un protocole d'échange de clés comme celui de Diffie-Hellman). Afin de limiter les attaques de type *Man-in-the-middle* dans la suite du protocole (on suppose que sk n'est pas compromise), on propose de rajouter à chaque message m échangé entre C et S un identifiant supplémentaire de la forme $H(sk||m)$. Ainsi, chaque message échangé entre C et S est maintenant de la forme

m	$H(sk\|\|m)$

Montrez que ce processus n'est absolument pas sécurisé dans le sens où un attaquant peut modifier le message m de sorte à obtenir un paquet valide entre C et S.